What is claimed is:

1. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving a user identification of a user from a card reader which obtains the user identification from an ID card containing same;

(b) determining whether there exists an authentication rule associated with the user based on the user identification received from the card reader;

(c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists;

(d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist;

(e) capturing the biometric information;

(f) retrieving a stored biometric information associated with the user identification;

(g) comparing the captured biometric information with the retrieved biometric information; and

(h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information.

2. The method of claim 1, prior to step (b), further comprising the steps of:

determining whether there exists an authentication rule associated with a remote computer from which the user is logging on;

prompting the user to provide biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists.

3. the method of claim 1, prior to step (b), further comprising the steps of:

determining whether there exists an authentication rule associated with an object to which the user is being authenticated for access;

prompting the user to provide biometric information according to the authentication rule associated with the object if it is determined that the authentication rule associated with the object exists.

4. The method of claim 1, after step (c) and prior to step (d), further comprising the steps of:

determining whether there exists an authentication rule associated with a group to which the user belongs:

prompting the user to provide biometric information according to the authentication rule associated with the group if it is determined that the authentication rule associated with the group exists;

wherein step (d) includes prompting the user to provide biometric information according to the system default authentication rule associated if it is determined that both the authentication rule associated with the user and the authentication rule associated with the group do not exist.

5. The method of claim 1, further comprising the steps of:

determining whether there exists an authentication rule associated with an object to which the user is being authenticated for access;

requesting the user to provide biometric information according to the authentication rule associated with the object if it is determined that the authentication rule associated with the object exists;

determining whether there exists an authentication rule associated with a remote computer from which the user is logging on if the authentication rule associated with the object to which the user is being authenticated for access does not exist;

requesting the user to provide biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists;

wherein step (b) includes determining whether there exists an authentication rule associated with the user if the authentication rule associated with the remote computer does not exist;

determining whether there exists an authentication rule associated with a group to which the user belongs if it is determined that the authentication rule associated with the user does note exist;

requesting the user to provide biometric information according to the authentication rule associated with the group if it is determined that the authentication rule associated with the group exists;

wherein step (d) includes prompting the user to provide biometric information according to the system default authentication rule if it is determined that both the authentication rule associated with the user and the authentication rule associated with the group do not exist.

6. The method of claim 1, wherein the biometric information includes information relating to one or more of a finger, hand, face, voice and signature of the user.

7. The method of claim 1, wherein the rule includes a parameter that specifies which type of biometric information reading devices is allowable for authentication.

8. The method of claim 1,wherein the rule includes a parameter that specifies the confidence level of a match between the captured biometric information and the retrieved biometric information.

9. The method of claim 1 further comprising interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.

10. The method of claim 9 wherein the ID card is interacted with the card reader by swiping the ID card through the card reader.

11. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving a user identification of a user from a card reader which obtains the user identification from an ID card containing same;

(b) determining whether there exists an authentication rule associated with the user based on the user identification received from the card reader;

(c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and

(d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exists.

12. The method of claim 11, prior to step (b), further comprising the steps of:

determining whether there exists an authentication rule associated with a remote computer from which the user is logging on;

authenticating the user with the captured biometric information and the previously stored biometric information according to the authentication rule associated with the remote computer if it is determined that the authentication rule associated with the remote computer exists.

13. The method of claim 11 further comprising interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.

14. The method of claim 13 wherein the ID card is interacted with the card reader by swiping the ID card through the card reader.

15. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs;

(b) determining whether there exists an authentication rule associated with the user based on the first user identification received from the card reader;

(c) if it is determined that the authentication rule associated with the user exists, prompting the user to provide biometric information according to the authentication rule associated with the user and proceeding to step (e), and if is determined that the authentication rule associated with the user does not exist, determining whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader;

(d) if it is determined that the authentication rule associated with the group to which the user belongs exists, prompting the user to provide biometric information according to the authentication rule associated with the group and proceeding to step (e), and if it is determined that the authentication rule associated with the group also does not exist, prompting the user to provide biometric information according to a system default authentication rule and proceeding to step (e);

(e) capturing the biometric information;

(f) retrieving a stored biometric information associated with the applicable authentication rule;

(g) comparing the captured biometric information with the retrieved biometric information; and

(h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information.

16. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving first and second user identification of a user from a card reader which obtains the user identifications from an ID card containing same, the first user identification identifying the user and the second user identification identifying a group to which the user belongs;

(b) determining whether there exists an authentication rule associated with the user based on the first user identification received from the card reader and if so, authenticating the user with a captured biometric information and previously stored biometric information according to the authentication rule associated with the user;

(c) if is determined that the authentication rule associated with the user does not exist determining whether there exists an authentication rule associated with a group to which the user belongs based on the second user identification received from the card reader, and if so authenticating the user with a captured biometric information and previously stored biometric information according to the authentication rule associated with the group;

(d) if it is also determined that the authentication rule associated with the group does not exist, authenticating the user with a captured biometric information and previously stored biometric information according to the authentication rule associated with a system default authentication rule.

17. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same;

(b) determining whether there exists an authentication rule associated with the user based on the user identification received from the keyboard or the card reader;

(c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists;

(d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist;

(e) capturing the biometric information;

(f) retrieving a stored biometric information associated with the user identification;

(g) comparing the captured biometric information with the retrieved biometric information; and

(h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information.

18. The method of claim 16 further comprising one of (i) typing in the user identification through the keyboard and (ii) interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.

19. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same;

(b) determining whether there exists an authentication rule associated with the user based on the user identification received from the keyboard or the card reader;

(c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and

(d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exists.

20. The method of claim 19 further comprising one of (i) typing in the user identification through the keyboard and (ii) interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.

21. A method of controlling access in a computer network environment comprising the steps of:

(a) automatically generating a user identification of a user;

(b) determining whether there exists an authentication rule associated with the user based on the automatically generated user identification;

(c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists;

(d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist;

(e) capturing the biometric information;

(f) retrieving a stored biometric information associated with the user identification;

(g) comparing the captured biometric information with the retrieved biometric information; and

(h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information.

22. A method of controlling access in a computer network environment comprising the steps of:

(a) automatically generating a user identification of a user;

(b) determining whether there exists an authentication rule associated with the user based on the automatically generated user identification;

(c) authenticating the user with a captured biometric information and a previously stored biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists; and

(d) authenticating the user with a captured biometric information and a previously stored biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exists.

23. A method of controlling access in a computer network environment comprising the steps of:

(a) receiving a user identification of a user from one of (i) a keyboard into which the user identification is typed, and (ii) a card reader which obtains the user identification from an ID card containing same;

(b) determining whether there exists an authentication rule associated with the user based on whether the user identification is received from the keyboard or the card reader;

(c) prompting the user to provide biometric information according to the authentication rule associated with the user if it is determined that the authentication rule associated with the user exists;

(d) prompting the user to provide biometric information according to a system default authentication rule if it is determined that the authentication rule associated with the user does not exist;

(e) capturing the biometric information;

(f) retrieving a stored biometric information associated with the user identification;

(g) comparing the captured biometric information with the retrieved biometric information; and

(h) completing a log-on procedure if the captured biometric information corresponds to the retrieved biometric information.

24. The method of claim 21 further comprising one of (i) typing in the user identification through the keyboard and (ii) interacting an ID card containing the user identification with the card reader whereby the card reader obtains the user identification.